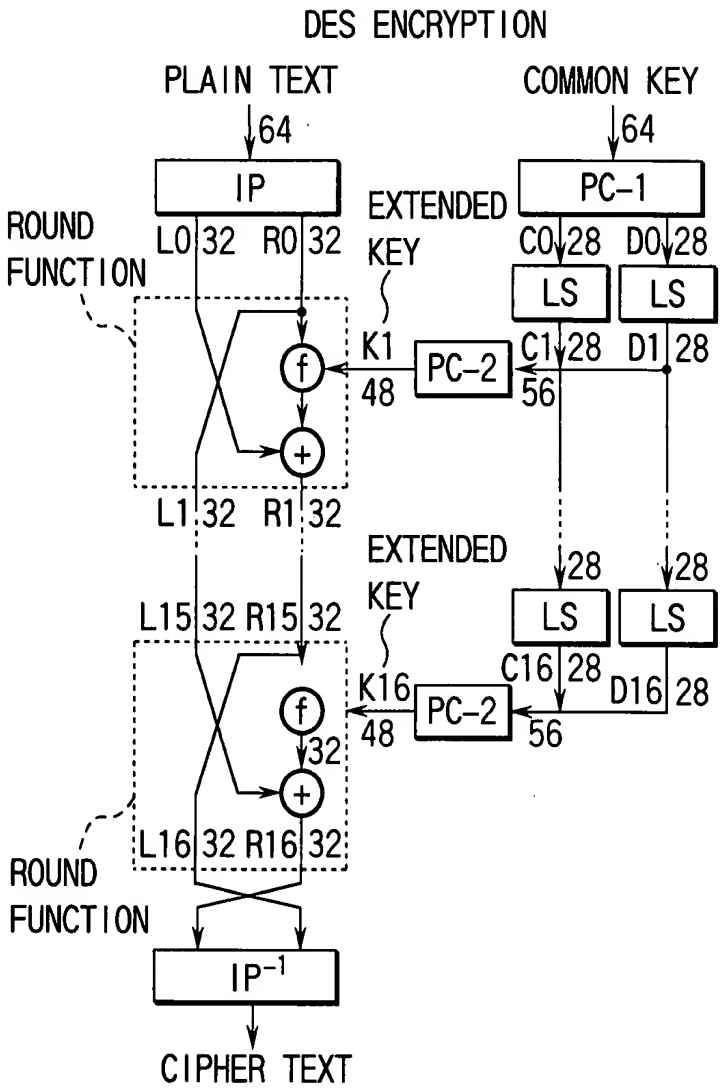

FIG. 1A

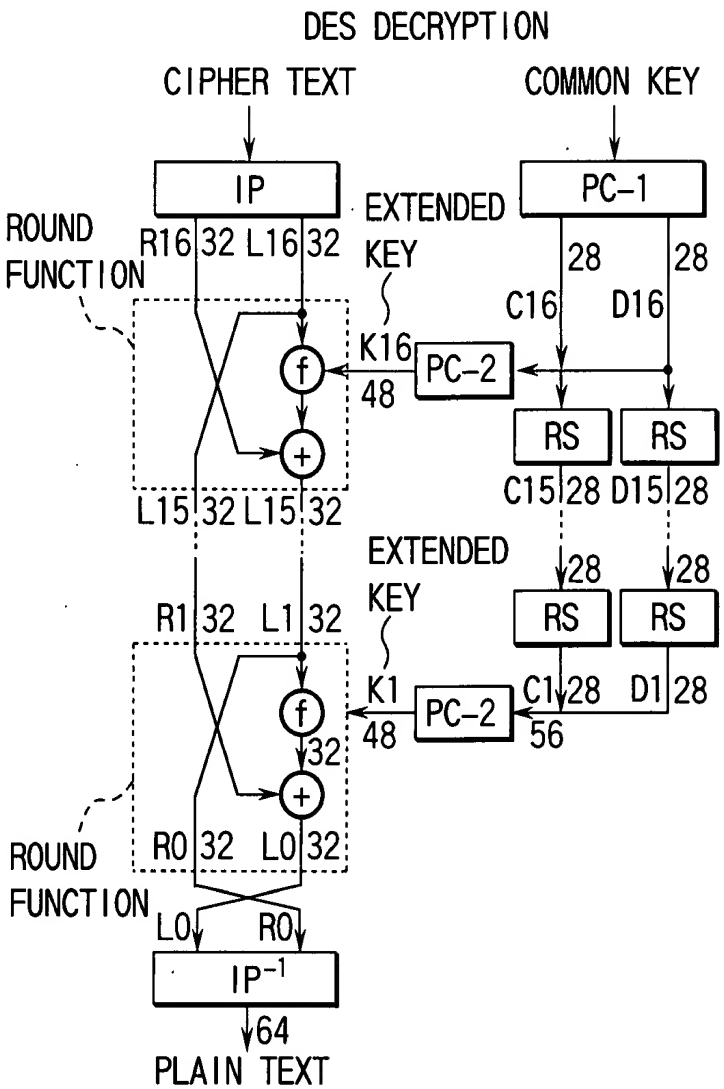

FIG. 1B

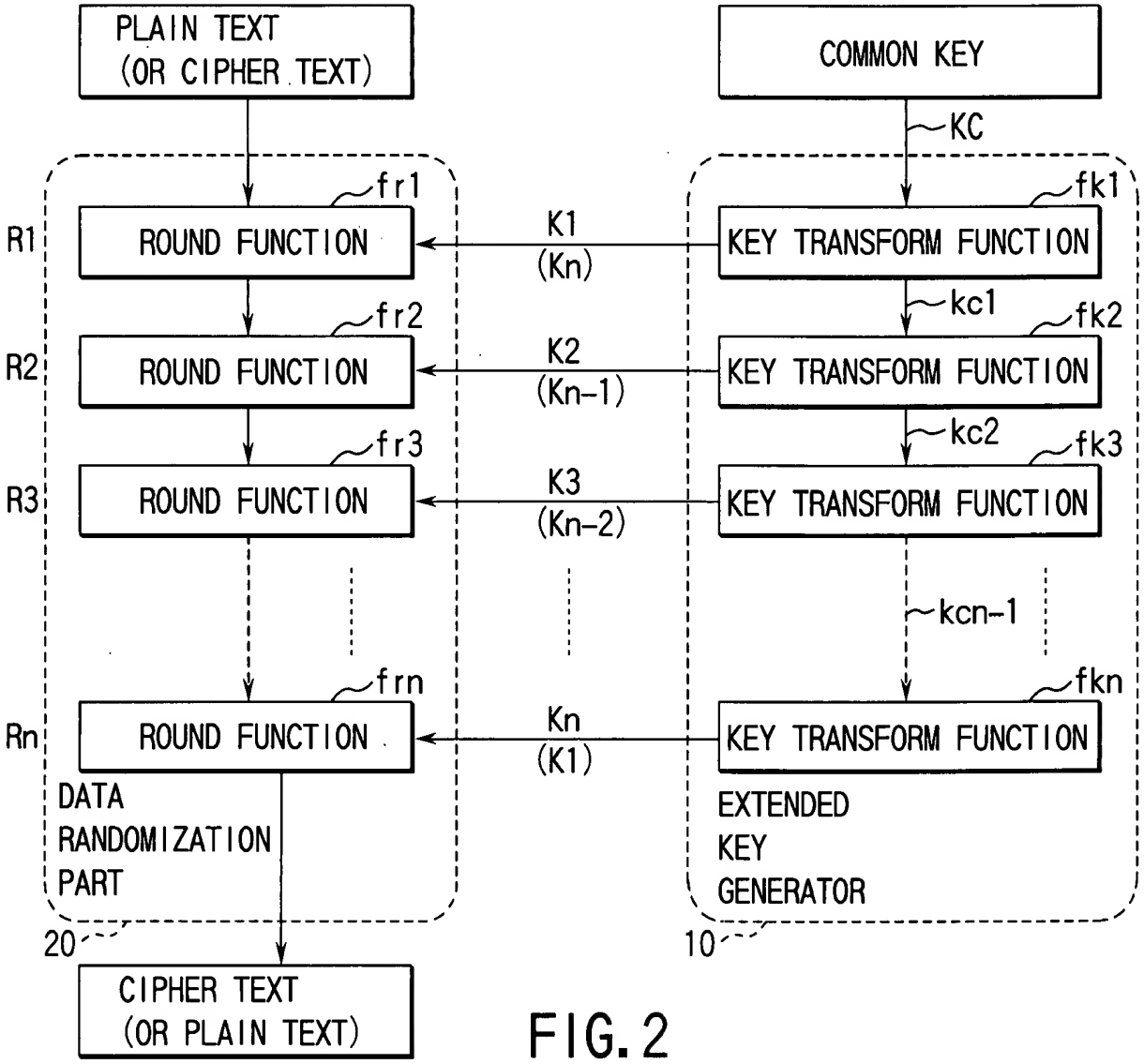
PLAIN TEXT
(OR CIPHER TEXT)
COMMON KEY
KC
fr1
fk1
R1
ROUND FUNCTION
K1
(Kn)
KEY TRANSFORM FUNCTION
kc1
fr2
fk2
R2
ROUND FUNCTION
K2
(Kn-1)
KEY TRANSFORM FUNCTION
kc2
fr3
fk3
R3
ROUND FUNCTION
K3
(Kn-2)
KEY TRANSFORM FUNCTION
kcn-1
frn
fkn
Rn
ROUND FUNCTION
Kn
(K1)
KEY TRANSFORM FUNCTION
DATA
RANDOMIZATION
PART
EXTENDED
KEY
GENERATOR
20
10
CIPHER TEXT
(OR PLAIN TEXT)

FIG. 2

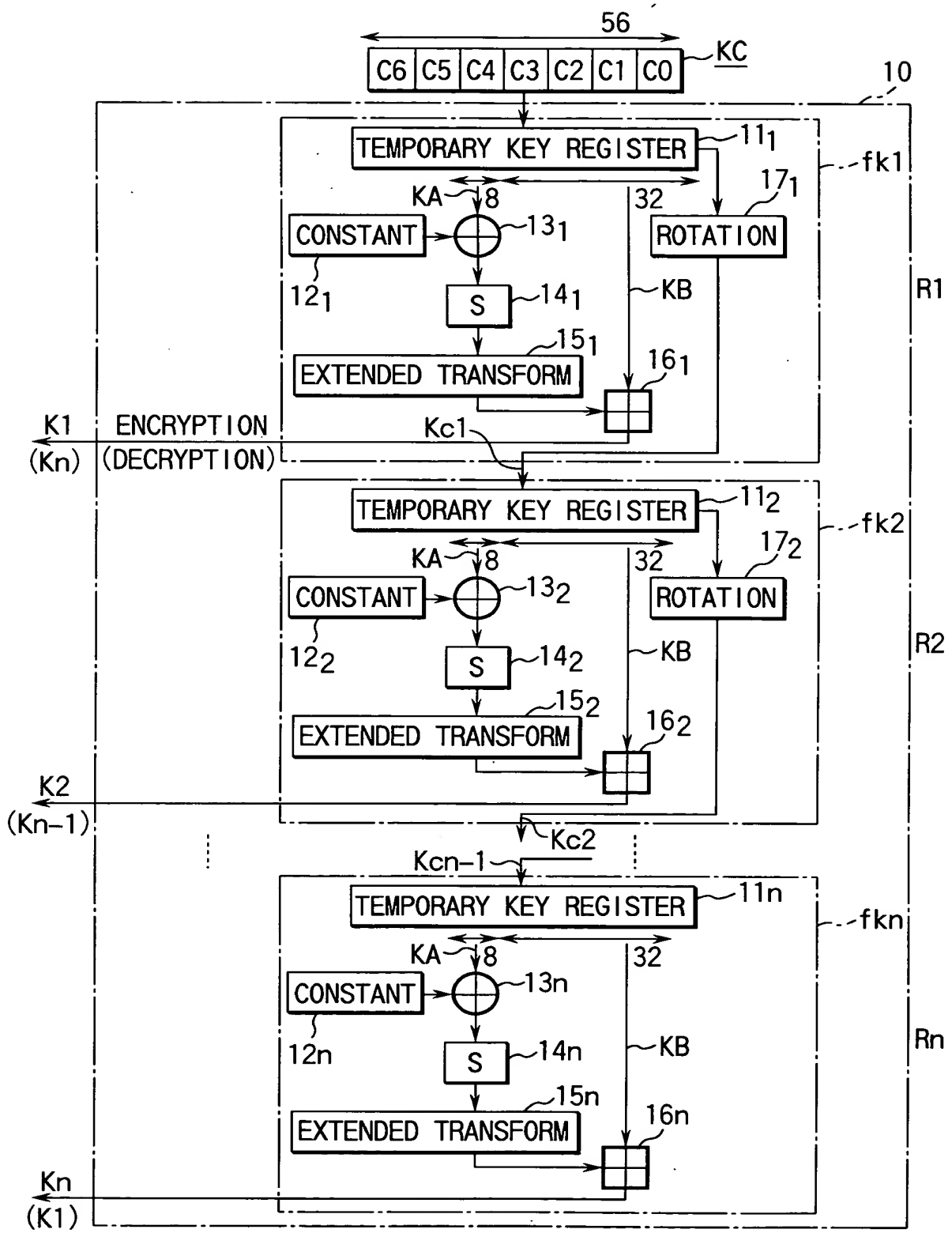
56
C6 C5 C4 C3 C2 C1 C0
KC
10
TEMPORARY KEY REGISTER
11 1
fk1
KA
8
32
17 1
CONSTANT
13 1
ROTATION
12 1
S
14 1
KB
R1
15 1
EXTENDED TRANSFORM
16 1
K1
(Kn)
ENCRYPTION
(DECRYPTION)
Kc1
TEMPORARY KEY REGISTER
11 2
fk2
KA
8
32
17 2
CONSTANT
13 2
ROTATION
12 2
S
14 2
KB
R2
15 2
EXTENDED TRANSFORM
16 2
K2
(Kn-1)
Kc2
Kcn-1
TEMPORARY KEY REGISTER
11n
fkn
KA
8
32
CONSTANT
13n
12n
S
14n
KB
Rn
15n
EXTENDED TRANSFORM
16n
Kn
(K1)

FIG. 3

KEY TRTANSFORM FUNCTION fki	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
VALUE OF CONSTANT REGISTER	0	1	2	3	4	5	6	7	7	6	5	4	3	2	1	0

FIG. 4A

KEY TRTANSFORM FUNCTION fki		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
VALUE OF CONSTANT REGISTER	ENCRYPTION	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	DECRYPTION	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

FIG. 4B

48,	54,	216,	182,	175,	5,	130,	229,	107,	52,	86,	11,	12,	221,	14,	15,
59,	4,	41,	140,	22,	164,	7,	89,	124,	81,	225,	176,	101,	66,	30,	118,
126,	242,	44,	211,	18,	161,	249,	105,	222,	174,	141,	202,	34,	103,	87,	233,
71,	49,	187,	51,	39,	1,	91,	77,	181,	172,	55,	42,	199,	79,	62,	194,
64,	72,	68,	133,	190,	158,	165,	232,	231,	115,	186,	116,	217,	240,	129,	171,
74,	169,	204,	173,	57,	58,	93,	17,	159,	245,	241,	155,	92,	156,	94,	26,
132,	82,	109,	230,	227,	28,	131,	209,	170,	25,	106,	73,	85,	98,	128,	143,
237,	108,	160,	61,	21,	179,	254,	197,	38,	122,	235,	70,	125,	31,	40,	102,
246,	119,	207,	53,	214,	111,	63,	135,	184,	236,	138,	56,	19,	29,	213,	88,
144,	145,	243,	127,	148,	137,	189,	151,	78,	153,	123,	183,	114,	157,	255,	252,
33,	6,	147,	163,	84,	97,	166,	167,	192,	0,	10,	208,	117,	196,	9,	16,
27,	206,	177,	104,	195,	83,	24,	75,	150,	203,	188,	50,	100,	69,	20,	180,
134,	193,	168,	8,	251,	247,	149,	201,	200,	112,	43,	142,	139,	205,	212,	37,
60,	226,	210,	154,	239,	80,	244,	215,	3,	120,	45,	23,	67,	99,	219,	223,
250,	220,	191,	32,	185,	253,	121,	13,	36,	228,	96,	162,	136,	46,	238,	146,
110,	178,	152,	2,	90,	234,	95,	65,	248,	113,	224,	35,	76,	218,	198,	47,

FIG. 5

NUMBER OF ROUNDS	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
ENCRYPTION (LEFT ROTATION)	9	9	11	11	13	13	13	10	13	13	13	11	11	9	9	
DECRYPTION (RIGHT ROTATION)	9	9	11	11	13	13	13	10	13	13	13	11	11	9	9	
KEY TRANSFORM FUNCTION fki	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	

FIG.6

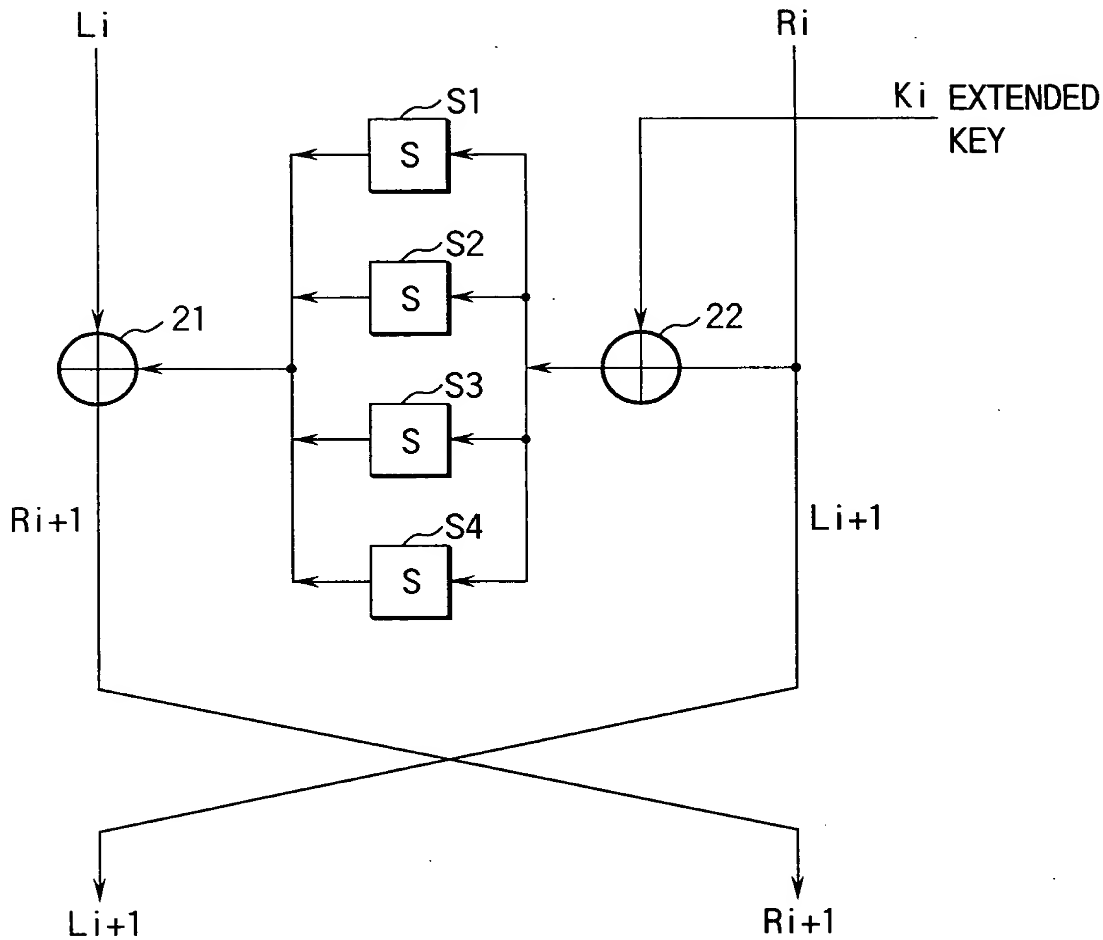

FIG. 7

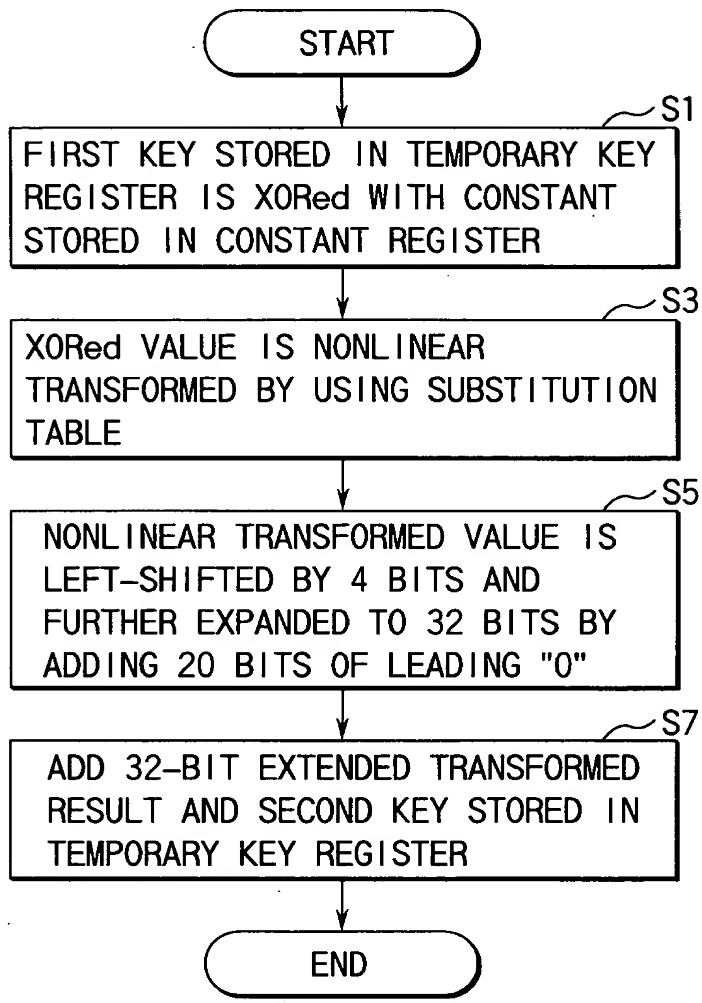

FIG. 8

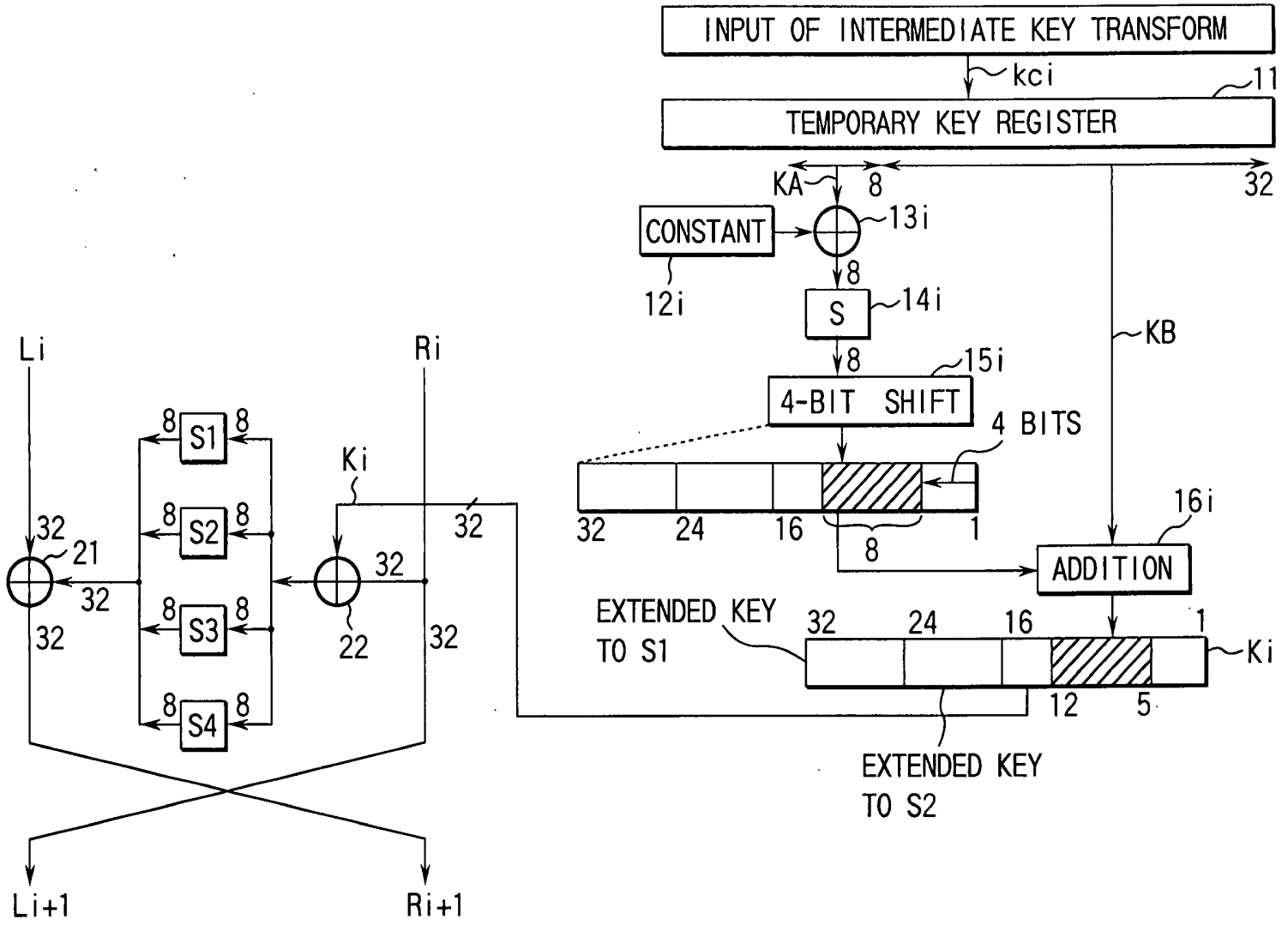
INPUT OF INTERMEDIATE KEY TRANSFORM
kci
11i
TEMPORARY KEY REGISTER
KA
8
32
CONSTANT
13i
12i
8
S
14i
KB
8
15i
4-BIT SHIFT
4 BITS
32
24
16
1
8
16i
ADDITION
EXTENDED KEY
TO S1
32
24
16
1
Ki
12
5
EXTENDED KEY
TO S2
Li
Ri
Ki
32
32
21
32
32
32
22
32
8
S1
8
8
S2
8
8
S3
8
8
S4
8
Li+1
Ri+1

FIG. 9

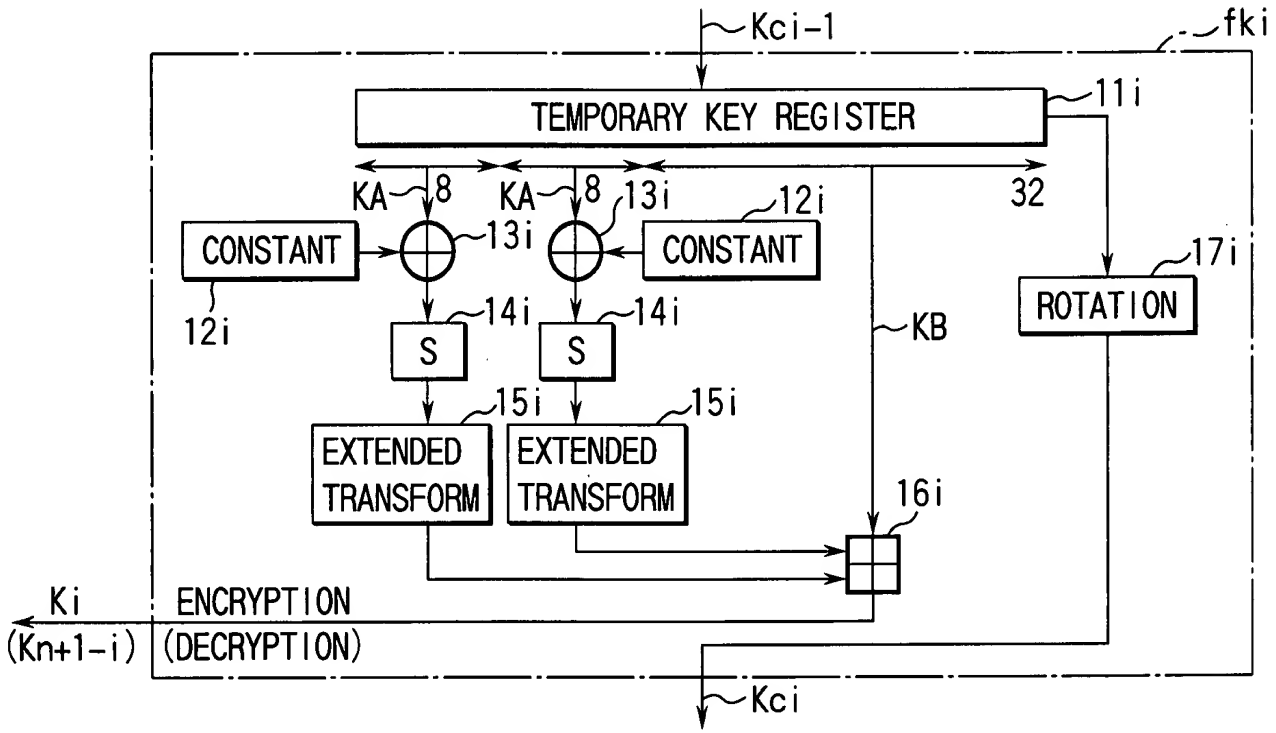
Kci-1
fki
TEMPORARY KEY REGISTER
11i
KA
8
KA
8
13i
12i
32
CONSTANT
13i
CONSTANT
17i
12i
14i
14i
ROTATION
KB
S
S
15i
15i
EXTENDED TRANSFORM
EXTENDED TRANSFORM
16i
Ki
(Kn+1-i)
ENCRYPTION
(DECRYPTION)
Kci

FIG. 10

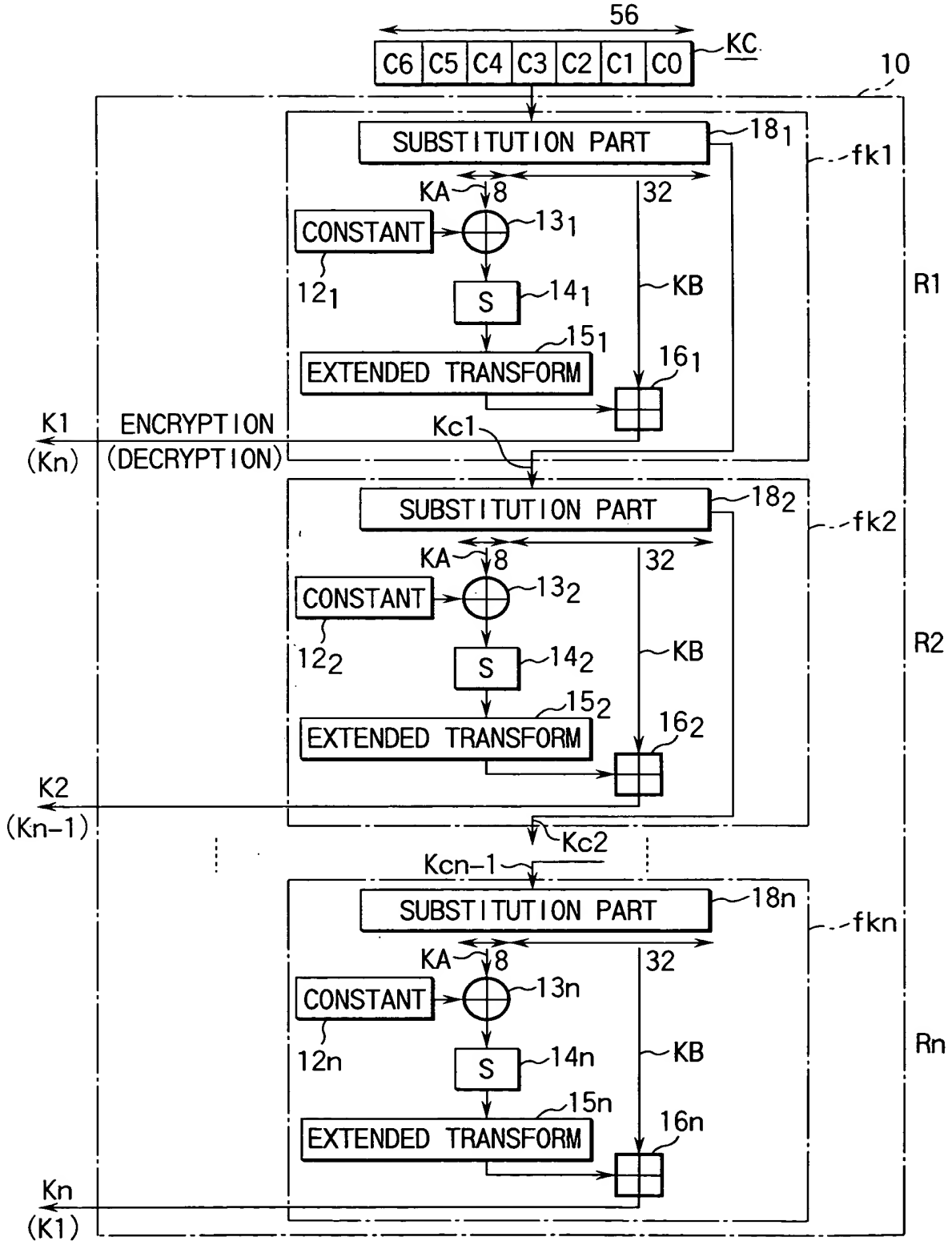

FIG. 11

NUMBER OF ROUNDS		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
PERMUTATION INPUT PROCESS	ENCRYPTION	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16
	DECRYPTION	$P16^{-1}$	$P15^{-1}$	$P14^{-1}$	$P13^{-1}$	$P12^{-1}$	$P11^{-1}$	$P10^{-1}$	$P9^{-1}$	$P8^{-1}$	$P7^{-1}$	$P6^{-1}$	$P5^{-1}$	$P4^{-1}$	$P3^{-1}$	$P2^{-1}$	$P1^{-1}$

FIG. 12

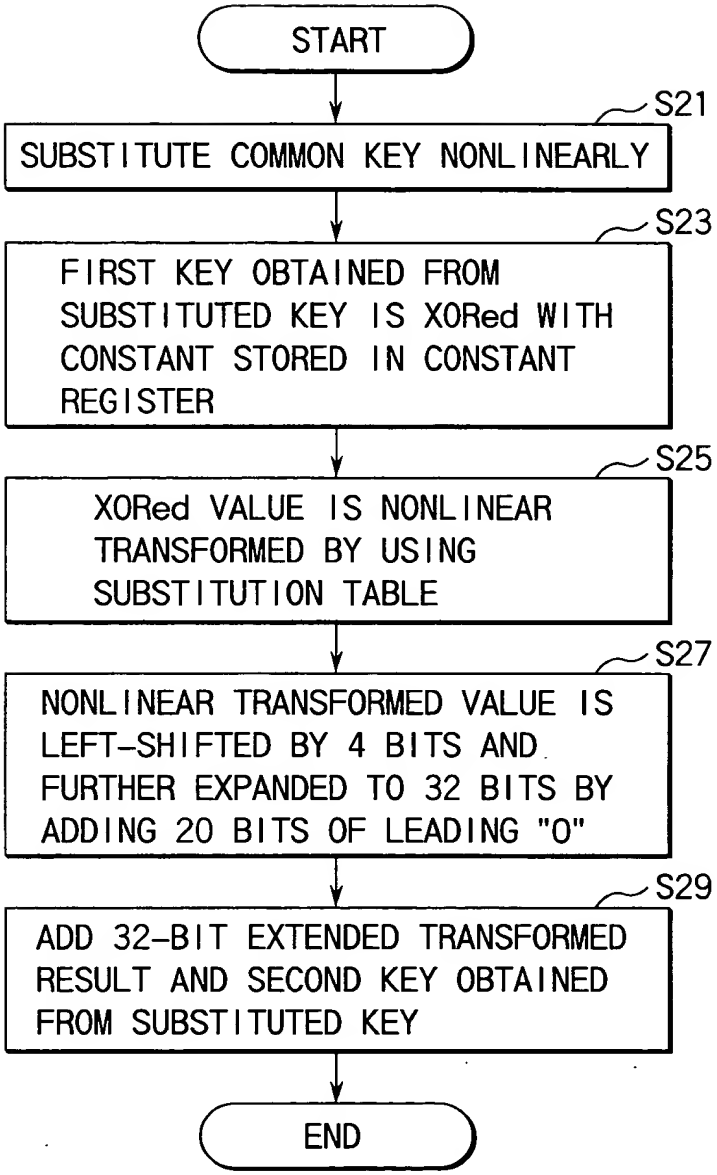

FIG. 13

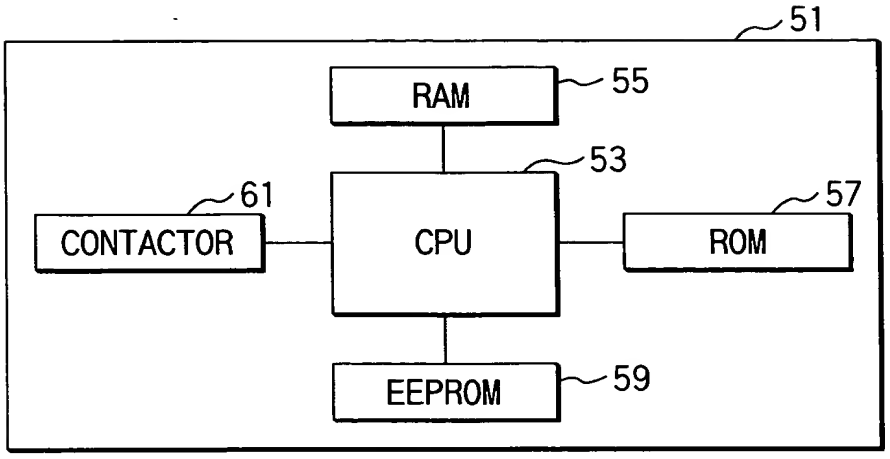

FIG. 14

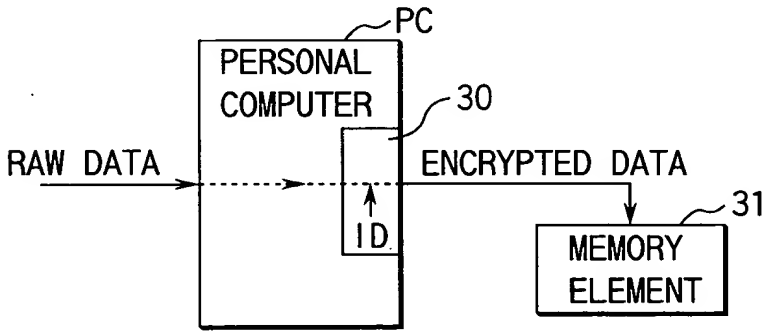

FIG. 15

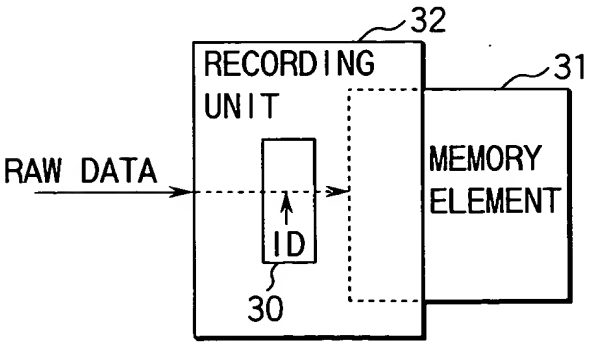

FIG. 16

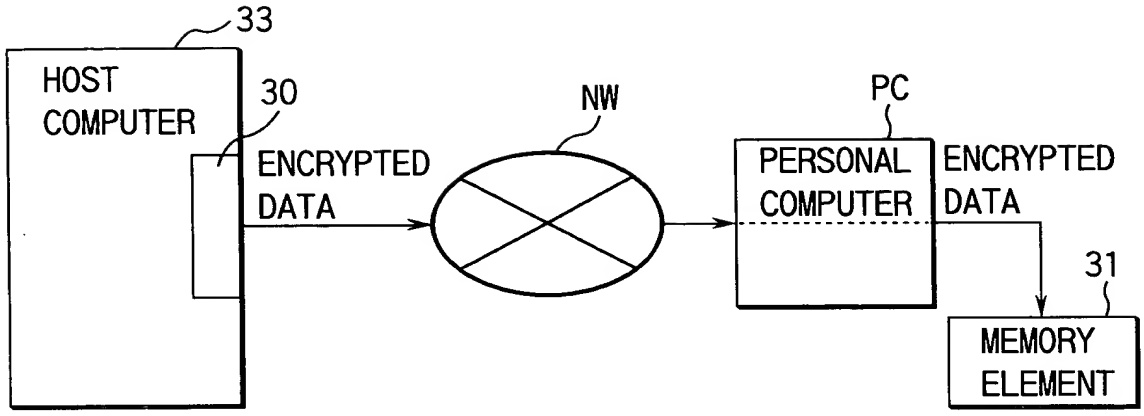

FIG. 17

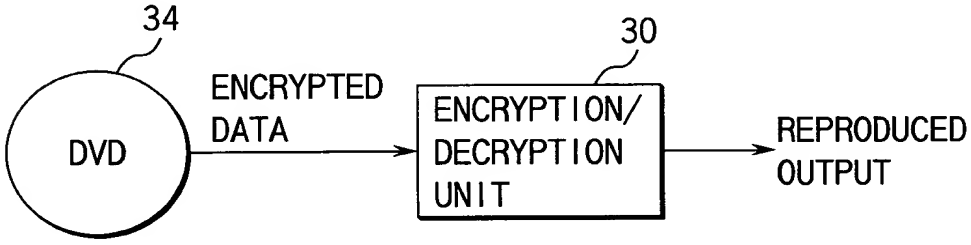

FIG. 18A

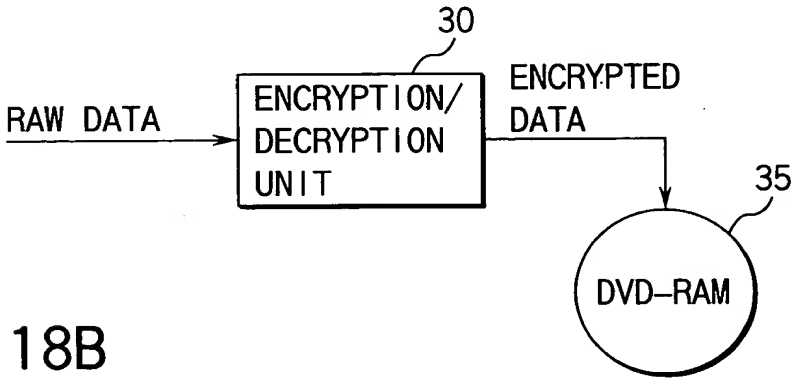

FIG. 18B